UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/902,520	07/10/2001	Jose' C. Brustoloni		7438

7590 03/21/2006

Docket Administrator
Lucent Technologies Inc.
Room 3J-219
101 Crawfords Corner Rd.
Holmdel, NJ 07733-3030

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/902,520	BRUSTOLONI, JOSE' C.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-18 and 20-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6-18 and 20-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on December 5, 2005. Claims 1,3-4,6-18, and 20-34 are currently being considered.

Response to Arguments

2. Applicant's arguments with respect to claims 1,3-4,6-18, and 20-34 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 and 18 are rejected under 35 U.S.C. 103(a) as being anticipated by Bendinelli et al. (U.S. Patent Publication No. 2002/0029276) in view of Rabenko et al. (U.S. Patent No. 6,765,913) in further in view of Ylonen (U.S. Patent No. 6,795,917).

4. With respect to claims 1 and 18, Bendinelli et al. disclose a method in program code used with a computer readable media (paragraphs 0019 and 0020) comprising:

- After a secure tunnel

(In paragraph 0180 line 12, Bendinelli discloses that the tunnel uses the IPSEC security protocol, meaning that the tunnel is secure.)

has been created between a first endpoint and a second endpoint on a packet network

(In paragraph 0138, Bendinelli discloses that after the tunnels are created, encryption algorithms and authentication algorithms are negotiated. In paragraph 0245, Bendinelli then discloses that one of these algorithms is SSL.)

which tunnel traverses at least one network address translator (NAT) that implements a heuristic methodology in translating addresses and/or port numbers, where the heuristic methodology is a methodology in which the NAT translates a private address of the first endpoint to a global address and then attempts to forward to the first endpoint packets sent by the second endpoint to the global address which global address is not uniquely associated with the first endpoint and where such attempts may fail due to collisions and/or race conditions

(paragraph 0141, lines 5- 13; In the third paragraph of the Linux VPN Masquerade website admitted as prior art by applicant, it states that VPN Masquerade is a part of IP Masquerade which enables to use IPSec-based VPN clients. In paragraph 0141, lines 14-17, Bendinelli discloses that IP Masquerade will be facilitated for use with NAT, after disclosing an environment using VPN and IPSec.),

and which tunnel is operating under a secure protocol that is independent of whatever applications are running on the first and second endpoints

(In paragraph 0180 line 12, Bendinelli discloses that the tunnel uses the IPSEC security protocol.)

and before one or more packets containing application data are sent between the first and second endpoints, sending a control packet from the first endpoint of the tunnel through the tunnel to the second endpoint of the tunnel; and

Waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint before sending packets containing application data through the tunnel.

(Bendinelli discloses that his method utilizes the SSL (Secure Sockets Layer) protocol handshake (Paragraph 0245, line 7) in which the client sends a control message to the sender and after receiving the message the server responds. This send and response of control packets continue in a specific manner as detailed in the SSL Version 3 specification and then the client and server have completed the handshake and may send data packets. An overview of the handshake protocol can be found in Section 5.5.)

Bendinelli does not explicitly disclose eliminating race conditions and collisions or providing automatic recovery from them.

Rabenko et al. further disclose the method or automatic recovery (column 9, line 6-8) wherein the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint. Rabenko et al. additionally further disclose the method wherein if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts

establishing a new tunnel (column 97, lines 19-37). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the recovery methods of Rabenko et al. with the system of Bendinelli in order to provide automatic recovery from a NAT crash or race conditions, as described in applicant's specification.

Furthermore, Bendinelli-Rabenko do not explicitly disclose noting a packet's security association identifier and using it to map the endpoint addresses. Ylonen states that some NATs may also recognize the security protocol such as IPSec and perform mappings on the SPI values in the packets (column 12 lines 17-23). Furthermore, Ylonen discloses changing the SPI values to that of the original value that was recorded (column 12 lines 17-23). Bendinelli discloses a NAT mechanism which implements IPSec, though does not explicitly disclose the use of the security parameter index (SPI) values to map the packets to the correct endpoint. However, it would have been obvious to one of ordinary skill in the art at the time of invention, to perform the recording and mapping of the SPIs as disclosed in Ylonen so that IPSec can still be used across NATs, so that "packet authentication can still be achieved securely in the presence of address translations and/or protocol converstions" (column 4 lines 33-37).

5. With respect to claims 3, and 20, Bendinelli et al. disclose further the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the tunnel is a secure tunnel and uses the IPSec security protocol suite. (In

paragraph 0180 line 12, Bendinelli discloses that the tunnel uses the IPSec security protocol, meaning that the tunnel is secure).

6. With respect to claims 4 and 21, Bendinelli et al. disclose further the method in program code used with a computer readable media (paragraph 0019 and 0020) wherein the tunnel use ESP in tunnel mode (In paragraph 0349, Bendinelli discloses the format of the IPSec packet and header. The description given matches with the ESP tunnel mode implementation of the IPSec security protocol suite as disclosed in Section 3.1 of RFC 2406 of the IETF, in which when ESP is employed, protection is offered only to the inner header, not to the IP packet's outer header and other layers as in AH).

7. With respect to claims 6 and 23, Bendinelli et al. disclose further the method in wherein the first endpoint is a client and the second endpoint is a server (paragraph 123).

8. With respect to claims 7 and 24, Bendinelli et al. further disclose the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the NAT implements VPN masquerade (In the third paragraph of the Linux VPN Masquerade website admitted as prior art by applicant, it states that VPN Masquerade is a part of IP Masquerade which enables to use IPSec-based VPN clients. In paragraph 0141, lines 14-17, Bendinelli discloses that IP Masquerade will be facilitated for use with NAT, after disclosing an environment using VPN and IPSec).

9. With respect to claims 8 and 25, Bendinelli et al. disclose a method in which program code used with a computer readable media (paragraphs 0019 and 0020) comprising:
sending a control packet from a first endpoint of a tunnel through the tunnel to a second endpoint of the tunnel (paragraphs 0389, lines 7-9) and waiting at the first endpoint for a responsive control packet through the tunnel from the second endpoint (paragraph 0389, lines 9-10) before sending packets other than a control packet through the tunnel (paragraphs 0389, lines 18-20). Bendinelli further discloses that the control packets being sent through the tunnel are ICMP packets (paragraph 0389, lines 7-9).

10. With respect to claims 9, 10, 26 and 27, Bendinelli et al. further disclose the method in program code used with a computer readable media (paragraphs 0019 and 0020) wherein the tunnel is defined by an epoch, the epoch comprising one security association (SA) in each direction, each SA having a negotiated limited lifetime, wherein before the end of the tunnel's lifetime the endpoints establish a new tunnel between them, and defining the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and with a security parameters index (SPI) chosen by the SA's destination.
(It is inherent in the usage of IPSEC and ESP in tunnel-mode in claims 3 and 4 that security associations must also be used (RFC 2401 from the IETF, Section 4). By using the tunnel to communicate from and to the gateway, it is inherent

that security associations were established in both directions (RFC 2401 from the IETF, Section 4.1, lines 6-8). It is also inherent in a security association to have negotiated authentication and/or encryption keys (RFC 2461 from the IETF, page 21 , bullet 5) with a security parameters index SPI (RFC 2401 from the IETF, Section 5.2, paragraph 2, lines 1-2) chosen by the destination (RFC 2401 from the IETF, Section 4.7, lines 1-3). Additionally, it is inherent in a security association utilizing ESP to have a negotiated limited lifetime wherein before the end of the tunnel's lifetime, the security association is rekeyed with a new SPI and the endpoints have in essence established a new tunnel (RFC 2401 from the IETF, page 21 , bullet 7, explanation of lifetimes).

11. Claims 11-12, 14, 15, 28-29, 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U.S. Publication 2002/0029276) as applied to claims 1-4 and 18-21 above, and further in view of Rabenko et al. (U.S. Patent No. 6,765,913) in further in view of Ylonen (U.S. Patent No. 6,795,917).

12. Bendinelli et al. disclose the limitations set forth in claims 1-4 and 18-21, upon which claims 1 1-12, 14-15, 28-29, 31, and 32 are dependent. However, Bendinelli et al. do not disclose the limitations set forth in claims 1 1-12 (or the corresponding claims 26-29).

Bendinelli et al. further do not disclose the limitations set forth in claims 14 and 15 (or corresponding claims 31 and 32).

Rabenko et al. disclose the limitations set forth in claims 1 1-12, 14-15, 28-29, 31,

and 32.

13. Bendinelli et al. , Ylonen, and Rabenko et al. are analogous art because both are in the field of secure data communications networks.

14. With respect to claim 11 and 28, Rabenko et al. further disclose the method in a computer readable medium (column 9, lines 6-8) wherein a designated endpoint has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish the tunnel (column 19, lines 37-41 , 44-48).

15. With respect to claim 12 and 29, Rabenko et al. further disclose the method in a computer readable medium (column 9, lines 6-8) wherein the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets (column 97, lines 16-19).

16. It would have been obvious to one of ordinary skill in the ad at the time of the invention to combine these teachings of Rabenko et al. with the method of Bendinelli et al. in order to reduce the possibility of race conditions, as described in applicant's specification.

17. With respect to claims 14, 15, 31, and 32, Rabenko et al. further disclose the

method in a computer readable medium (column 9, lines 6-8) wherein the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint. Rabenko et al. additionally further disclose the method wherein if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts establishing a new tunnel (column 97, lines 19-37).

18. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the recovery methods of Rabenko et al. with the system of Bendinelli in order to provide automatic recovery from a NAT crash or race conditions, as described in applicant's specification.

19. Claims 13 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U. S. Publication 2002/0029276) as applied to claims 1 and 18 above, in view of Ylonen (U.S. Patent No. 6,795,917) and further in view of Capurka et al. (U. S. Patent 6,678,258).

20. Bendinelli et al. , Ylonen, and Capurka et al. are analogous art because they all deal with the field of packet data communication systems.

21. With respect to claims 13 and 30, Bendinelli et al. did not disclose the method in computer readable medium wherein if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends through the tunnel a control packet to the second endpoint.
Capurka et al. further disclose the method in computer readable medium (column 3, lines 48-53) wherein if the first endpoint does not receive any packets through the tunnel for a predetermined time interval then the first endpoint sends through the tunnel a control packet to the second endpoint (column 2, lines 65-67 to column 3, line 1).

22. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Bendinelli et al. with the method of Capurka et al. in order to provide a more inexpensive and efficient recovery method (column 1, lines 49-52).

23. Claims 11-12, 14, 15, 28-29, 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U.S. Publication 2002/0029276) as applied to claims 1-4 and 18-21 above, and further in view of Rabenko et al. (U.S. Patent No. 6,765,913) in further in view of Ylonen (U.S. Patent No. 6,795,917).

24. Bendinelli et al. disclose the limitations set forth in claims 1-4 and 18-21, upon which claims 1 1-12, 14-15, 28-29, 31, and 32 are dependent. However, Bendinelli et al. do not disclose the limitations set forth in claims 1 1-12 (or the

corresponding claims 26-29).

Bendinelli et al. further do not disclose the limitations set forth in claims 14 and 15 (or corresponding claims 31 and 32).

Rabenko et al. disclose the limitations set forth in claims 1 1-12, 14-15, 28-29, 31, and 32.

25. Both Bendinelli et al. and Rabenko et al. are analogous art because both are in the field of secure data communications networks.

26. With respect to claim 11 and 28, Rabenko et al. further disclose the method in a computer readable medium (column 9, lines 6-8) wherein a designated endpoint has responsibility for establishing the new tunnel and ignores requests initiated by the other endpoint to establish the tunnel (column 19, lines 37-41 , 44-48).

27. With respect to claim 12 and 29, Rabenko et al. further disclose the method in a computer readable medium (column 9, lines 6-8) wherein the second endpoint waits for a packet from the first endpoint through the tunnel before using the tunnel to send any packets (column 97, lines 16-19).

28. It would have been obvious to one of ordinary skill in the ad at the time of the invention to combine these teachings of Rabenko et al. with the method of

Bendinelli et al. in order to reduce the possibility of race conditions, as described in applicant's specification.

29. With respect to claims 14, 15, 31, and 32, Rabenko et al. further disclose the method in a computer readable medium (column 9, line 6-8) wherein the first endpoint sends through the tunnel to the second endpoint a predetermined maximum number of control packets without receiving any packets through the tunnel then the first endpoint establishes a new tunnel to the second endpoint. Rabenko et al. additionally further disclose the method wherein if an endpoint is unable to complete the establishment of a new tunnel before a predetermined time limit then that endpoint abandons establishment of that tunnel and starts establishing a new tunnel (column 97, lines 19-37).

30. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the recovery methods of Rabenko et al. with the system of Bendinelli in order to provide automatic recovery from a NAT crash or race conditions, as described in applicant's specification.

31. Claims 16,17,33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bendinelli et al. (U.S. Patent Publication No. 2002/0029276) in view of Rabenko et al. (U.S. Patent No. 6,765,931) in further in view of Ylonen (U.S. Patent

No. 6,795,917) as applied to claims 1-3,9-10,15,18,20,26,27, and 32 above, and further in view of Ogier et al. (U.S. Patent Publication No. 2003/0179742).

32. With respect to claims 16, 17, 33, and 34, Ogier et al. further disclose the method in a computer readable medium (The method is implemented in the internetworking system which is made up of subnets (paragraph 0053, lines 1-2), which are in turn made up of nodes (paragraph 0055, lines 6-10). Nodes, as disclosed by Ogier et al. in paragraph 0384, are a computer readable medium.) wherein if an endpoint successively fails to establish a new tunnel before a predetermined maximum number of times then that endpoint closes the connection currently being used to establish tunnels with the other endpoint and opens another such connection (paragraph 0361 , lines 1-12) wherein the connection is an IKE session (Bendinelli: paragraph 0187, lines 4-6), paragraph 0188, lines 6-9).

33. Bendinelli et al., Rabenko et al., Ylonen and Ogier et al. are all analogous ad because all deal with the field of secure data communications networks. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Ogier et al. with the combined system of Bendinelli et al. and Rabenko et al. in order to provide fail-over recovery from a crash of the NAT.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
03/15/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

CR 3/17/06